**Dobra praksa u bezbednosti informacija/ podataka**[[1]](#endnote-1)

Vaše preduzeće dužno je da zaštiti tehnologije i informacije od strateškog značaja. To obuhvata **„podatke u mirovanju“** (laptop i desktop računare, uređaje za čuvanje podataka, baze podataka, itd.); **„podatke u upotrebi“** (*SharePoin*t, *Cloud*, serveri sa datotekama i aplikacijama, itd.); i **„podatke u pokretu“** (elektronska pošta, prenos datoteka, itd.). **U nastavku teksta slede neki od primera dobrih praksi u bezbednosti informacija/ podataka:**

Laptop računari:

Napuštanje zemlje sa kontrolisanim tehničkim podacima ili informacijama na laptop računaru može da predstavlja kršenje propisa vaše zemlje o kontroli spoljne trgovine strateškom robom. Pomenute kontrole mogu da se prošire i obuhvate sve priloge i poruke u vašoj elektronskoj pošti ili datoteke na diskovima računara.

Kada se na laptop računarima nalaze kontrolisani podaci, vaše preduzeće treba da nastoji da obezbedi pribavljanje odgovarajućih dozvola nadležnih nacionalnih organa (ukoliko je primenljivo i potrebno), kao i odgovarajuće šifriranje datih podataka radi sprečavanja neovlašćenog pristupa.

**Dobra praksa kod međunarodnih putovanja**

* Definisati detaljne smernice i procedure za sastanke, međunarodna putovanja, elektronsku poštu, simpozijume, itd., na kojima se kontrolisani podaci na bilo koji način razmatraju.
* Uzdržati se od slanja kontrolisanih datoteka putem elektronske pošte ili uključivanja tehničkih podataka u tekstove poruka poslatih elektronskom poštom. Preporuka je da vaše preduzeće deli samo i isključivo datoteke putem linkova preko internih stranica koje zahtevaju sigurnosnu prijavu.
* Ne ostavljati elektronsku poštu i priloge sa kontrolisanim tehničkim podacima u fascikli elektronske pošte. Pohranite podatke na sigurnom serveru i pre odlaska obrišite tu elektronsku poštu sa vašeg laptop računara.
* Ne učitavati softvere na računare koji se nose na međunarodna putovanja.
* Obezbediti da se prenos elektronske pošte koja sadrži kontrolisane podatke vrši u šifriranom obliku i preko sigurnih servera koji se nalaze u vašoj zemlji.
* Po potrebi, vaše preduzeće bi trebalo da razmotri korišćenje virtuelne privatne mreže (VPN) za daljinski pristup kontrolisanim podacima van matične države. Napomena: *Upotreba VPN-a može da eliminiše potrebu za nošenjem kontrolisanih podataka ili informacija na laptop računarima zaposlenih.*

Elektronsko čuvanje kontrolisanih informacija/ podataka

Odgovarajuće čuvanje kontrolisanih informacija na serverima vašeg preduzeća i elektronskim uređajima za skladištenje podataka predstavlja važan deo osiguranja zaštite kontrolisanih podataka od neovlašćenog pristupa. Nenameran pristup neovlašćenih lica kontrolisanim podacima u određenim situacijama može da predstavlja kršenje nacionalnih propisa o kontroli spoljne trgovine strateškom robom.

Kontrolisane podatke od strateškog značaja moguće je zaštititi šifriranjem, lozinkama ili čuvanjem na lokacijama koje nisu na mreži.[[2]](#endnote-2)

**Dobre prakse za čuvanje elektronskih podataka**

* Ograničite skladištenje podataka na personalnim računarima ili zajedničkim serverima.
* Vodite spisak računara, mrežnih uređaja i uređaja za čuvanje podataka koji sadrže kontrolisane tehnologije i koji treba da uživaju veći stepen zaštite (npr. antivirusne provere, osposobljen zaštitni zid (*firewall*), zaključavanje sesije, šifriranje datoteka, jake lozinke). Od IT sektora zatražite postavljanje računara i uređaja sa primenjenim odgovarajućim merama zaštite.
* Računare u vašem preduzeću opremite opcijom automatske odjave sa sistema koja od korisnika zahteva da nakon određenog vremena ponovo unesu svoju lozinku za pristup sistemu.
* Obezbedite da serveri datoteka vašeg preduzeća imaju zaštitu naloga/ lozinke na nivou datoteka u direktorijumima podataka.
* Ograničite pristup osetljivim datotekama. Zaposleno lice odgovorno za kontrolu interne usklađenosti odnosno službenik za kontrolu tehnologije (TCO) u vašem preduzeću (ukoliko je primenljivo) ili glavni službenik/ direktor za usklađenost (CCO) treba da sastavi i redovno ažurira spisak svih zaposlenih sa ovlašćenjima za pristup osetljivim datotekama, i da taj spisak dostavi vašem IT sektoru.
* Ne koristite programe (kao na primer, *Microsoft Sharepoint, Dropbox* ili *Box*) za čuvanje ili slanje detoteka koje sadrže kontrolisane podatke.
* Koristite namenske uređaje za čuvanje podataka (prenosivi diskovi/ usb diskovi, itd.).
* Na odgovarajući način šifrirajte datoteke na prenosivim uređajima za čuvanje podataka. 
* Uspostavite procedure i smernice za uništavanje/ brisanje kontrolisanih tehnologija sa uređaja na kraju njihovog životnog veka (na primer, iz memorija, sa CD i DVD diskova, usb memorija).
1. Prilagođeno i modifikovano iz “Australian Best Practice Guide for the Management of Controlled Exports and Technology,” Australian Industry Group, May 2014.

 “University of Pennsylvania Office of Research Services TCP Template,” University of Pennsylvania.

 [↑](#endnote-ref-1)
2. [↑](#endnote-ref-2)